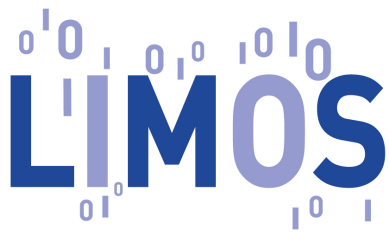

JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE
ARIANE TICHIT • SÉBASTIEN VARRETTE
LES
BLOCK CHAINS
EN 50 QUESTIONS
-
Comprendre le fonctionnement et les enjeux de cette technologie
DUNOD


JEAN-GUILLAUME DUMAS • PASCAL LAFOURCADE • ETIENNE ROUDEIX
ARIANE TICHIT • SÉBASTIEN VARRETTE
LES
NFT
EN 40 QUESTIONS
-
Des réponses claires et détaillées pour comprendre les Non Fungible Tokens
DUNOD

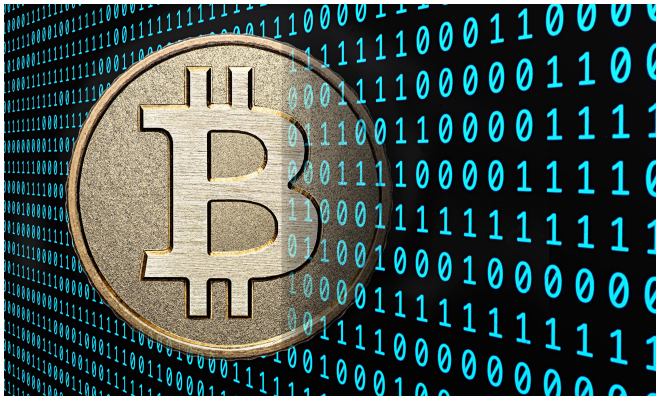
La Blockchain et Web3

Pascal Lafourcade

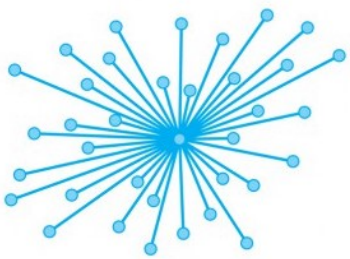


Valence
17 octobre 2023

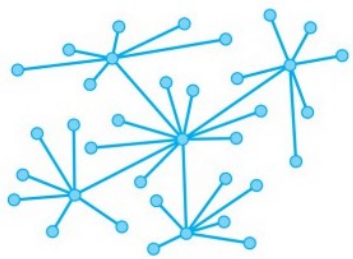
La révolution Bitcoin 2009



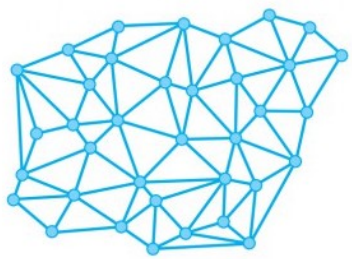
- Cryto-monnaie décentralisée et distribuée



Système centralisé



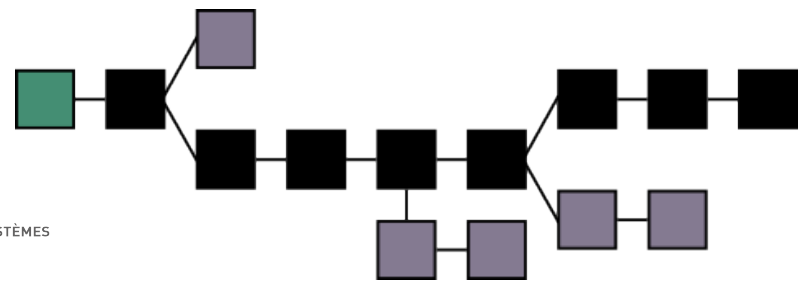
Système décentralisé



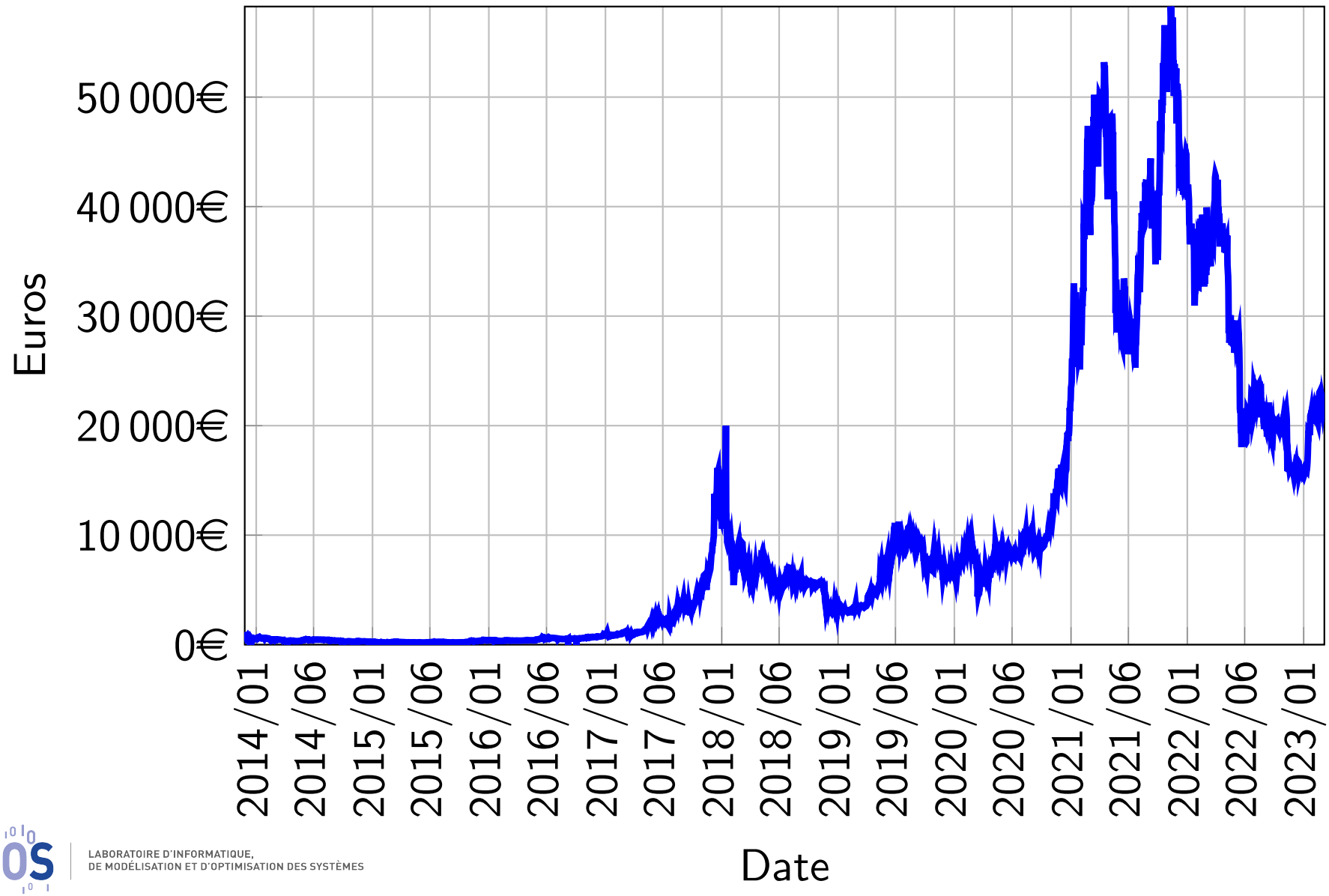
Système distribué

21 millions BTC

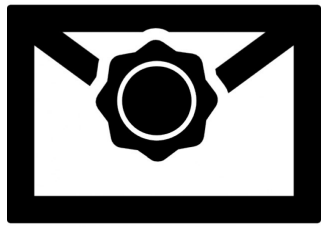
- Inarrêtable car distribuée
- Infalsifiable et auditable

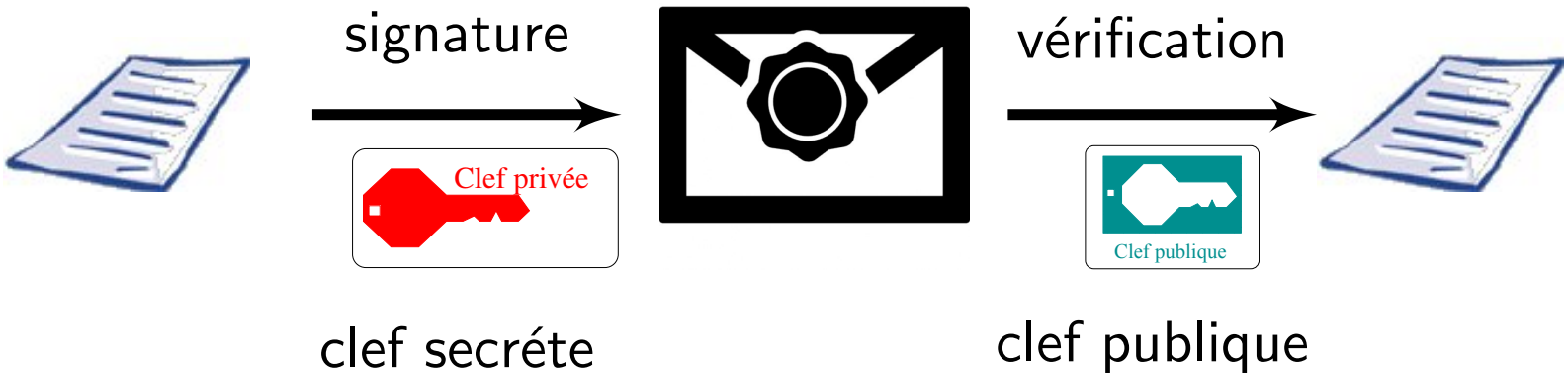


Taux de change du bitcoin



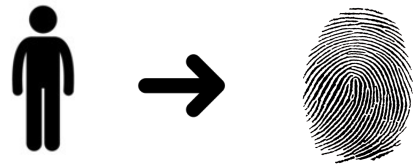
Signature





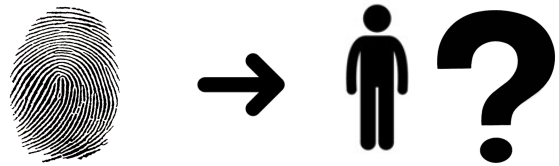
RSA: $m^d \mod n$

Fonction de Hachage (RIPEMD-160, SHA-256)

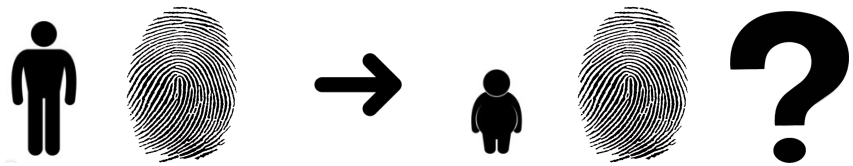


Propriétés de résistance

- Pré-image



- Seconde Pré-image

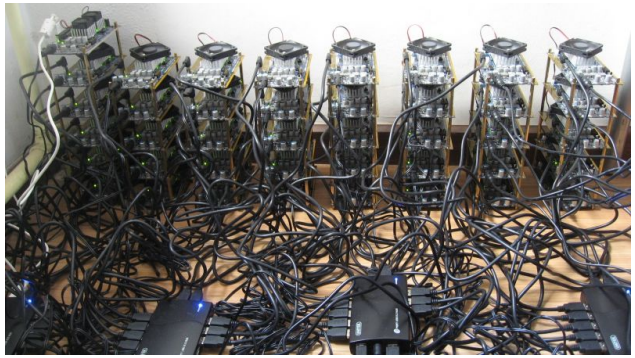


- Collision

Miner des Bitcoins

Miner des Bitcoins

Les “*mineurs*” valident les transactions contre des bitcoins



Miner des Bitcoins

- Valider = résoudre un **objectif de hachage**
- Récompense initiale 50 BTC pour une validation
- Divisée par 2 tous les 210000 validations

$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$

Miner : Objectif de hachage

Cible = 00000000000000000254845fa930deac4086b3e3bce21147e93f463b206d8076

Trouver une nombre n tel que

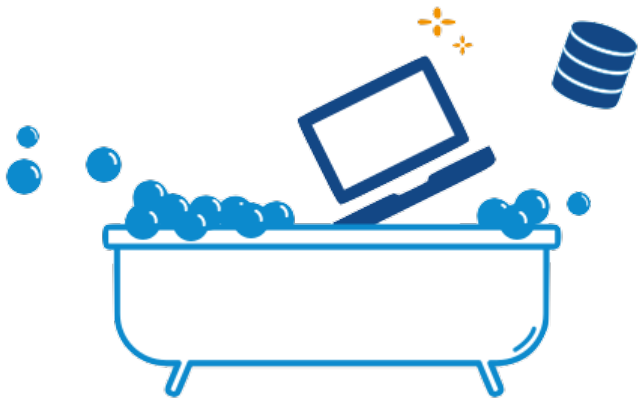
$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Cible}$$

Avoir au moins 18 zéros au début de x

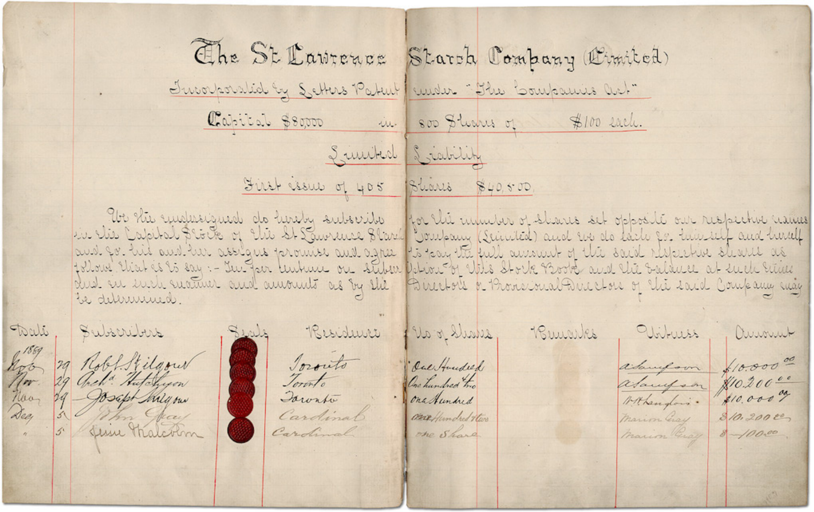
Stratégie : brute force

Tester toutes les valeurs possibles de n

Freins

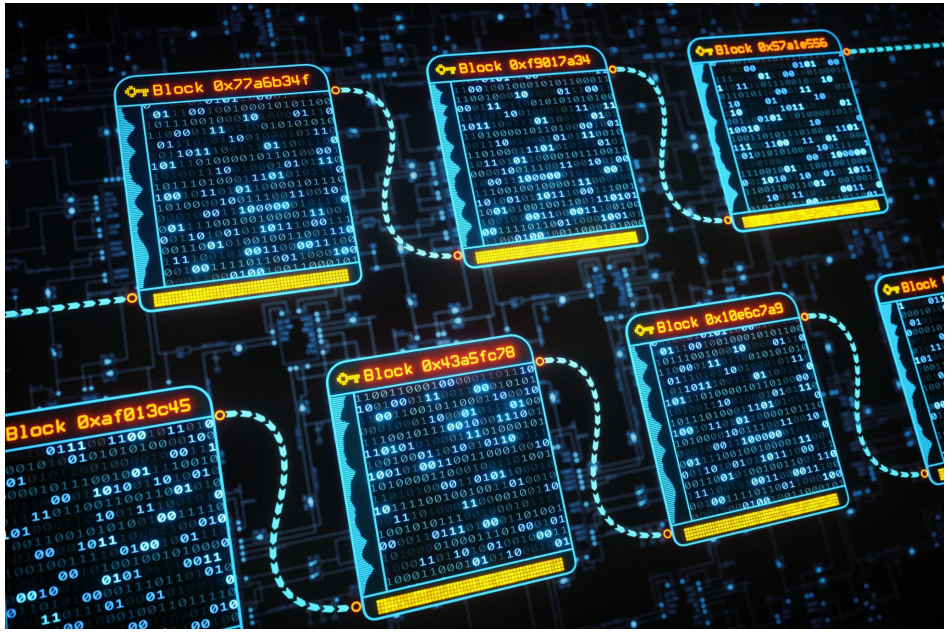


Blockchain



LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

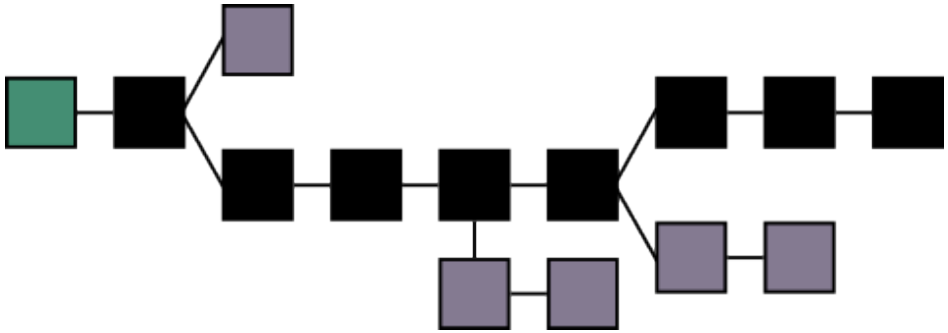
Blockchain



Registre distribué, sécurisé, infalsifiable

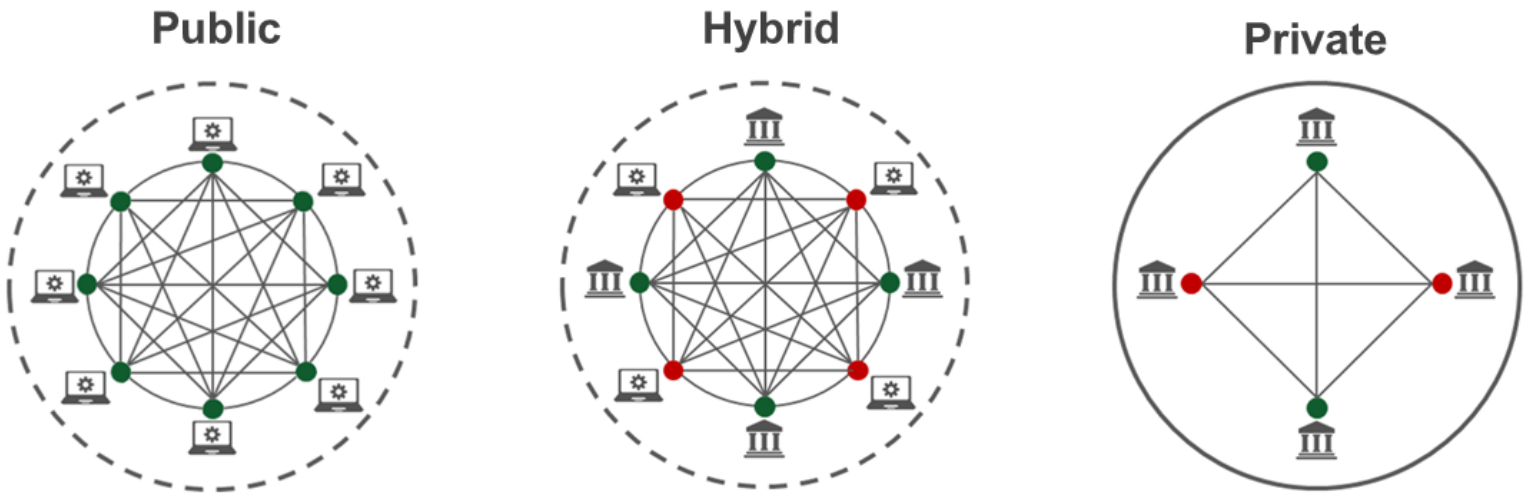
Mineurs valident des transactions

Tiennent à jour le registre distribué

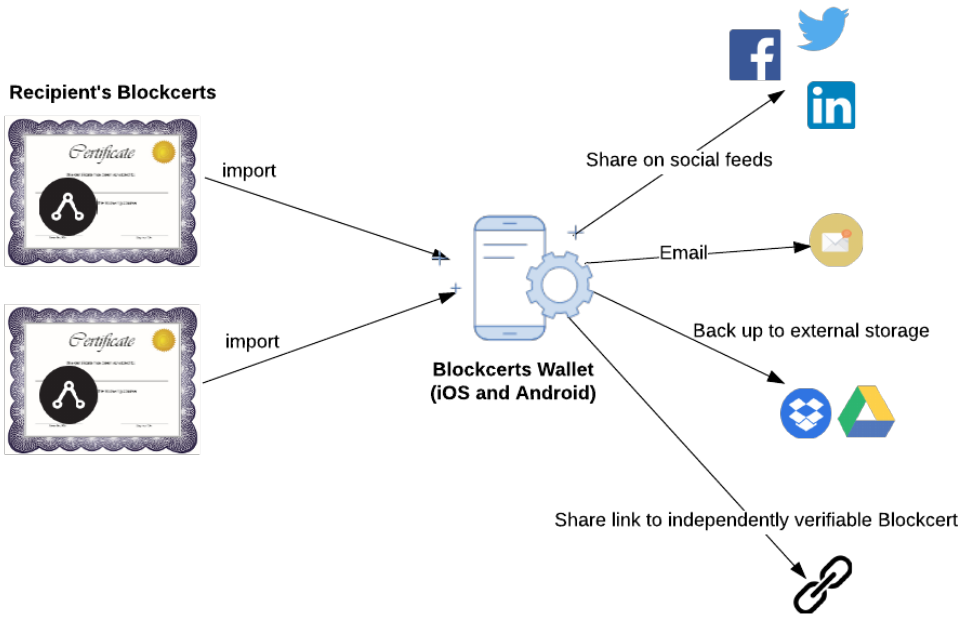


Inarrêtable, Infalsifiable, Auditable

Blockchain Privée vs Publique



Blockchain Application : MIT Diploma

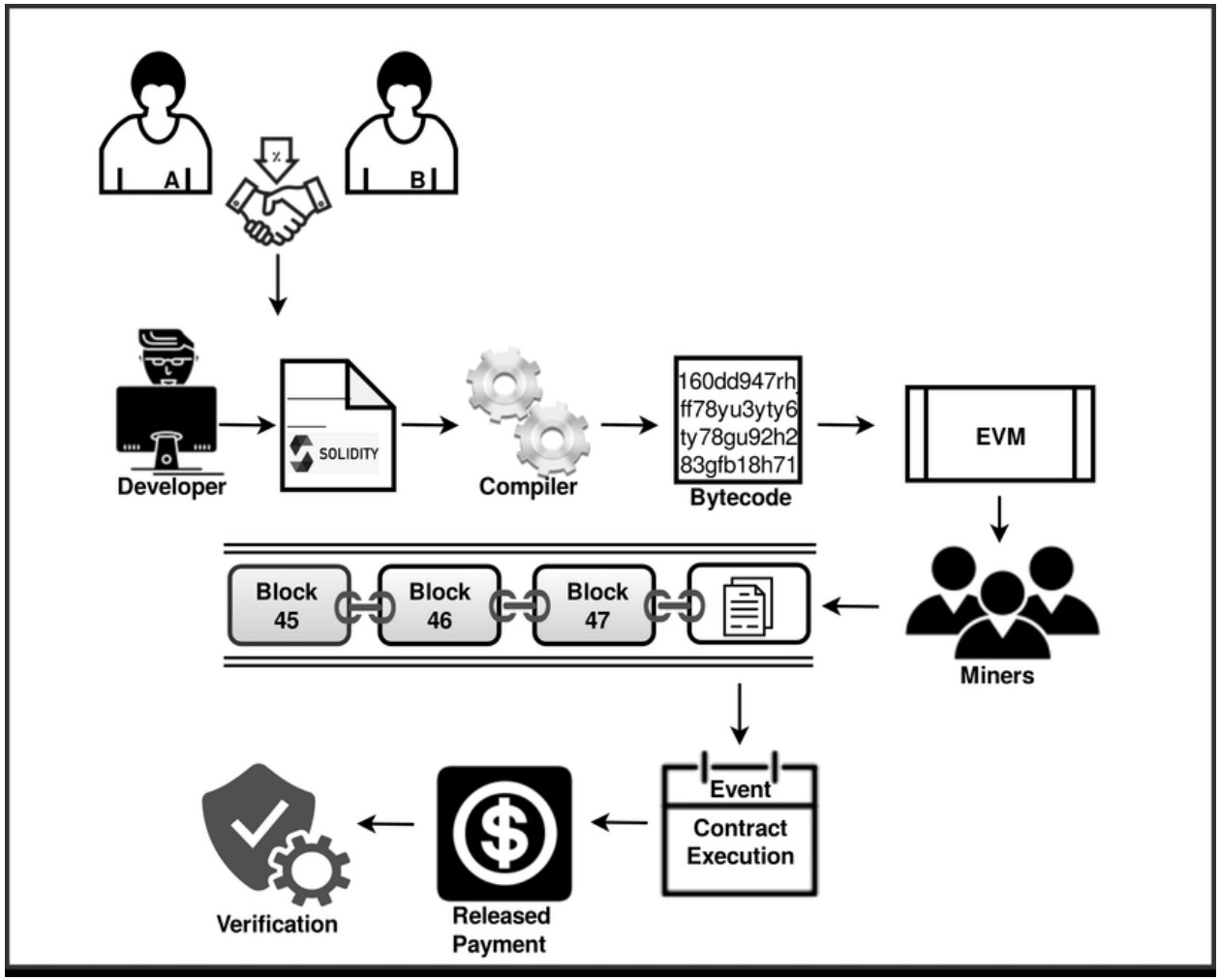


Blockchain Applications : Auction

Properties

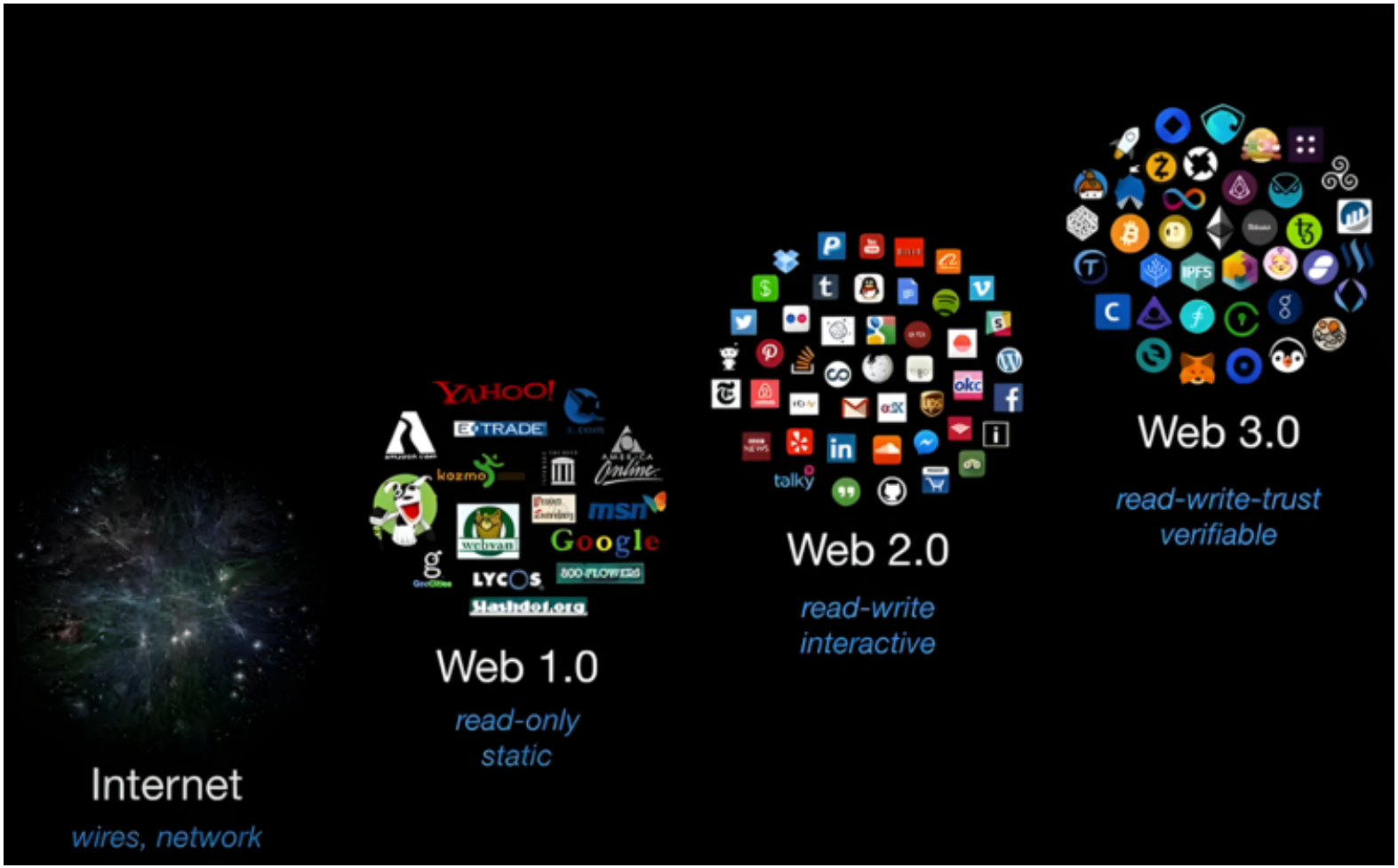
Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Spedning, Non-Repudiation ...

Smart Contract



Smart Contract

Internet to Web3

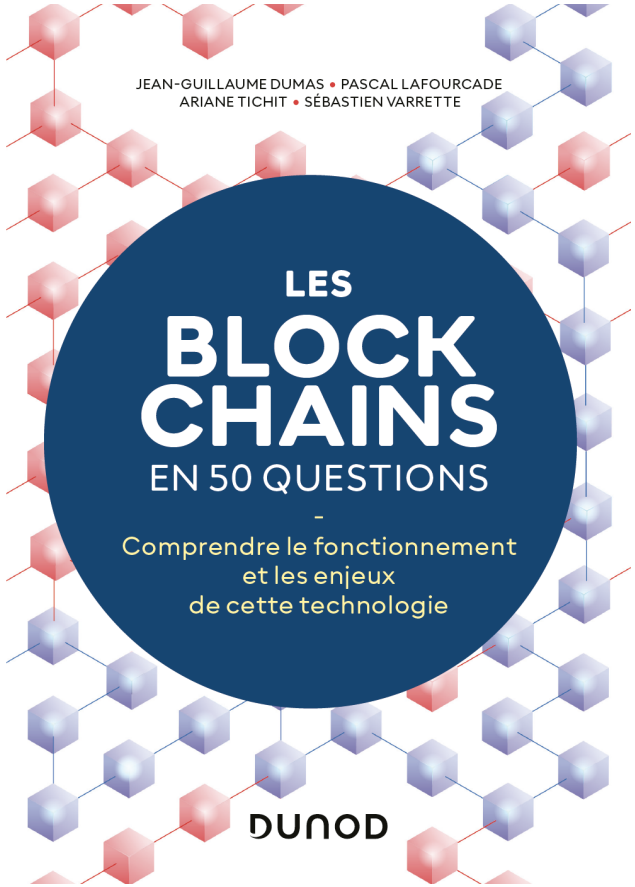


Choses à retenir

- La révolution Blockchain est en marche
- Un formidable outil
- De nombreuses applications mais bien comprendre les limites
- La cryptographie est au centre de la sécurité

Merci pour votre attention

Questions ?



pascal.lafourcade@uca.fr

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES